

RB

PEB: USAO201300232

16 - 23 63 JMC

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA

v.

MARTIN ROBERT HALL

*
*
*
*
*
*

CRIMINAL NO.

UNDER SEAL

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Christine D. Carlson, being duly sworn, depose and state:

INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) assigned to the Special Agent in Charge in Baltimore, Maryland. I have been so employed since June 1996. As part of my daily duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of search warrants, which involved child exploitation and/or child pornography offenses. I have received formal training from U.S. Customs, ICE, HSI and other agencies in the area of child pornography, pedophile behavior, collectors of other obscene material and Internet crime. As a federal agent, your Affiant is authorized to investigate

16 - 23 63 JMC

violations of laws of the United States and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

2. I am submitting this affidavit in support of a criminal complaint and arrest warrant for MARTIN ROBERT HALL ("HALL"), born in 1962, for violation of Title 18, United States Code, Sections 2252(a)(1) (Transportation of Child Pornography) and 2252A(a)(5)(B) (Possession of Child Pornography). The statements in this affidavit are based in part on information, documents, and reports prepared by the Baltimore County Police Department, and on my experience and background as a Special Agent of HSI. Since this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation.

DESCRIPTION OF THE NETWORK

3. The *Network* is a distributed, Internet-wide, peer-to-peer (P2P) network designed to allow anonymous and censorship resistant publication and distribution of information. The system is regularly used to distribute and download child sexual abuse (CSA) material. The *Network* is free and open source software. It uses decentralized, distributed data stores to store information, and has a suite of free software for working with this data store. Users contribute to the network by giving bandwidth and a portion of their hard drive (called the *datastore*) for storing files. Files are automatically kept or deleted depending on how popular they are, with the least popular being discarded to make way for newer or more popular content. Files are encrypted, so generally the user cannot easily discover what is in his data store. Chat forums, websites, and search functionality, are all built on top of this distributed data store.

4. The *Network* works by storing small encrypted blocks of content distributed on the computers of its users and connecting only through intermediate (proxy) computers which

pass on requests for content and sending them back without knowing the contents of the full file, similar to how routers on the Internet route packets without knowing anything about files. Except The *Network* provides caching, encryption, and does not rely on centralized structures. This allows users to anonymously publish or retrieve various kinds of information.

5. The *Network* can only be used to access content that has been previously inserted into the *Network*. The *Network* attempts to protect the anonymity of both subjects inserting data into the network (uploading) and those retrieving data from the network (downloading). Unlike other file sharing systems, there is no need for the subject uploading the file to remain on the network after uploading a file or group of files. Instead, during the upload process, the files are broken into blocks, or splits, and stored on a variety of other computers on the network. When downloading, those blocks are found and reassembled.

6. Unlike other P2P networks, the *Network* not only transmits data between nodes (nodes are computers running the *Network*) but actually stores data, working as a huge distributed cache. Files on the *Network* are split into multiple small blocks, with additional blocks added to provide redundancy. Each block is handled independently, meaning that a single file may have parts stored on many different nodes. An index to the complete file is contained in a high level block, called a manifest.

7. A user wishing to share a file "inserts" the file to the network. After insertion, or uploading, is finished, the user receives the key¹ to the file. The uploading node is then free to shut down, because the file is stored in the network. It will remain available for other users whether or not the original uploading node is online. No single node is responsible for the content; instead, it is replicated to many different nodes. However, there is no ability to search

¹ A "key" is a series of letters and numbers that is provided to the uploader by the network after the upload is complete. In order to download the file from the network after uploading, a user can cut and paste the "key" into a downloader that can access The *Network*.

for a file key that has been inserted into the network. The user sharing the file has to make the key available to other the *Network* users with something like email, or to a broader audience by posting it on a message board, forum, or on the *Network*.

8. The *Network* provides two (2) modes of operation, *OpenNet* and *DarkNet*. *OpenNet* makes connections to any other *OpenNet* node, or strangers. In *DarkNet* mode, connections are only made only to friends a user has previously exchanged node ids with, creating a closed network.

INVESTIGATION OF MARTIN ROBERT HALL

9. On or about August 12, 2016 while reviewing a law enforcement database of requests received by undercover law enforcement nodes, a Baltimore County Police detective observed IP address **96.244.150.210** routing and/or requesting suspected child pornography file blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requester of the file.

10. The detective observed that between August 11, 2016 at 18:16:08 UTC and August 17, 2016 at 10:59:07 UTC, a computer running the *Network* software, at IP address **96.244.150.210**, requested from the undercover law enforcement *Network* nodes - parts, or blocks, of files with SHA1 hash values the detective had previously downloaded from the *Network*. By way of example, two of files IP address **96.244.150.210** requested parts, or blocks of files from are described as follows:

- a. **VID 20150712 143254 1.avi** – this video file is approximately 3:25 minutes in length and depicts a nude prepubescent female lying on a bed with her legs spread open and her vagina visible. The prepubescent female's face is blurred out. An erect adult male's penis enters the screen and it appears that a person off camera, possibly another child, is masturbating the penis. The nude prepubescent female child then sits up, points at the erect penis, and then points at her vagina. The prepubescent female then lays back and the adult male touches and rubs the prepubescent female's vagina. The adult male then

16 - 23 63 JMC

proceeds to rub and push his penis against the prepubescent female's vagina and anus. This adult male slightly penetrates the prepubescent female's anus and then continues to rub his penis on her vagina until he ejaculates on her vagina.

- b. **VID 20150527 124900.avi** – this video file is approximately 1:03 minutes in length and depicts a prepubescent female naked from the chest down. The prepubescent female is seen touching and manipulating her vagina. An adult's hand reaches into view and begins to touch the prepubescent female's vagina. A mostly blurred out adult's face is then seen performing oral sex on the prepubescent female. The adult's hands are then seen touching and rubbing the prepubescent female's vagina and anus.

I have reviewed the above referenced files and determined they are child pornography as defined in Title 18, United States Code, Section 2256(8).

11. A subpoena was sent to Verizon requesting information, to include subscriber name and address, for IP address **96.244.150.210** from August 11, 2016 at 18:16:08 UTC to August 17, 2016 at 10:59:07 UTC, the dates and times the IP address was routing and/or requesting suspected child pornography file blocks. Verizon provided the following information:

Subscriber Name:	Belinda Hall
Service address:	6 Meadowsweet Ct. Reisterstown, MD 21136
Telephone #:	410-599-6237
Username:	martyhall
Email Address:	belindajanehall@gmail.com

12. On September 1, 2016, the detective prepared a search and seizure warrant for 6 Meadowsweet Ct. Reisterstown, MD 21136. The warrant was signed by the Honorable Judge Cavanaugh of the Baltimore County District Court.

13. On September 7, 2016, members of the Baltimore County Police Department, Crimes Against Children Unit executed the search and seizure warrant at 6 Meadowsweet Court, Reisterstown, Maryland. At the time the warrant was executed, Martin Hall and Belinda Hall were present.

14. Detective Josh Rees of the Baltimore County Police Department advised the Halls of their rights per *Miranda*, which they both stated they understood. Detective Rees learned that Martin Hall and Belinda Hall are the only occupants of the residence. When Detective Rees asked about the internet in the home, Martin Hall advised that he did not want to answer that question. At that time Detective Rees took Belinda Hall aside and spoke to her in private to ask about the computers at the residence. Mrs. Hall advised that all of her computers and devices were in her first floor office to the left of the front door. She advised that all of her husband's computers and devices were in his basement office. She advised that they do not use each other's computers/devices. Detective Rees asked Mrs. Hall if she uses the *Network* software, to which she replied that she does not even know what it is.

15. Martin Hall (hereinafter "HALL") was then interviewed in private and was again advised of his rights per *Miranda*. HALL stated that he understood his rights and agreed to be interviewed. The interview was audibly recorded. HALL admitted that he has used the *Network* software for a couple of years. HALL advised that he has uninstalled it, erased it, and reinstalled it several times. He advised that when he deletes it, he uses a wiping program called Eraser. HALL spoke in a very educated manner about how the *Network* operates and how to navigate different portions of the *Network*. HALL also talked about his use of the separate forum/message board software that operates on the *Network*. I know through training and knowledge that this particular forum/message board software is blatantly and commonly used by people to communicate about child pornography, child sexual abuse, and as a place to share access to and download files on the *Network*. HALL acknowledged that the computers and devices located in his basement office belong to him and that he is the only person who uses them. HALL confirmed that the Western Digital hard drive connected to his Dell laptop

16 - 23 63 JMC

computer is encrypted with True Crypt encryption software. HALL refused to provide Det. Rees with the encryption password.

16. In the basement office, detectives found a Dell desktop computer powered on and running with two external hard drives connected to it. There was also a Dell laptop located on the desk in the basement office that was powered on and had one external hard drive connected to it. Detectives also located a Dell SRS Premium Squad laptop on the desk that was powered off.

17. Detective Rees began an on-scene forensic triage of the Dell desktop computer by utilizing the tool OS Triage. A further on-scene forensic triage was conducted on this computer by Forensic Supervisor Kollmann utilizing Encase software along with write block hardware. Forensic Supervisor Kollmann located evidence that the *Network* software had been installed on the Dell desktop computer and was recently deleted. Supervisor Kollmann also located a file wiping program called Eraser on the Dell desktop computer.

18. Detective Raut utilized the forensic tool OS Triage to conduct a forensic triage of the Dell laptop that was powered on and located on the desk in the basement office. Detective Raut was immediately alerted to the presence of True Crypt encryption and the file wiping program Eraser. It was determined that the Western Digital external hard drive connected to this laptop was mounted as volume W: and was encrypted. OS Triage located thousands of images saved on the external hard drive under folders titled "travel" and "temp". The detectives found images of HALL engaged in sexual acts with Filipino woman of varying ages. Some of the females HALL was engaged in sexual acts with appeared to be young and the detectives were unable to determine if they were definitely adults. Many of these images were taken with a Canon EOS Rebel T2i digital camera. Detectives also located numerous images of what

16 - 23 63 JMC

appeared to be Filipino children, mostly young girls, dressed in minimal clothing taken with a Canon EOS Rebel T2i digital camera. Additionally, detectives located several nude images of what appeared to be prepubescent Filipino female child where the child is nude. The images show the child's face and her vagina. Some of the images are zoomed in on the child's vagina, thus making it the focal point of the image. These images were also taken with a Canon EOS Rebel T2i digital camera and three of the images depicting the same prepubescent female are described as follows:

- a. **august-1 006.jpg** – an image file depicting a naked prepubescent female standing in front of a green curtain. Metadata for this image indicates the image was taken on or about August 3, 2016 with a Canon EOS Rebel T2i digital camera.
- b. **atrium 1 012.jpg** – an image file depicting the same prepubescent female as described above. The prepubescent female is lying on a bed wearing a white tank top and white underwear. The white tank top is off one shoulder exposing her left breast and her underwear is pulled down to her mid-thigh exposing her genitalia. Metadata for this image indicates the image was taken on or about July 25, 2016 with a Canon EOS Rebel T2i digital camera.
- c. **atrium 1 011.jpg** – an image file depicting a close up of the same prepubescent minor as described above. This image is a close up of the prepubescent female's vagina. The prepubescent female's white underwear is pulled down exposing her genitalia to the camera. Metadata for this image indicates the image was taken on or about July 25, 2016 with a Canon EOS Rebel T2i digital camera.

19. Det. Rees showed HALL a facial picture of the naked prepubescent female as described above. HALL immediately stated that he knows her and that she is the sister of one of his "girlfriends", Ellen. HALL advised that her name is possibly Sandra and he thinks she is 12 or 13 years old. HALL denied taking the pictures, even though he admitted to knowing her and that the pictures were taken with the same camera he owns. HALL admitted to having traveled to the Philippines several times over the past 15 years. I know through my training and

16 - 23 63 JMC

experience that the Philippines is a well-known sex tourism destination for individuals interested in engaging in sexually explicit conduct with minors. Detectives located and seized a Canon EOS Rebel T2i digital camera containing an SD card in a backpack in HALL's basement office.

20. Detectives also seized HALL's U.S. passport from a black suitcase that was located in the basement office. Entry and exit stamps located within the passport indicate that HALL arrived in the Philippines on May 1, 2016 and departed the Philippines on August 10, 2016, which is the time frame when the images of the minor female described in paragraph 18 were produced. Additionally, HALL's wife told detectives that her husband had been in the Philippines from April 2016 until August 2016.

21. Based on the fact that images described above that were seized during this on-scene forensic exam were (1) produced during the period that HALL was in the Philippines, that (2) the images were taken with the same make and model camera that HALL owns and was recovered from his office, that (3) the pictures depict a prepubescent female that HALL admitted is the younger sister of one of his Filipino "girlfriends", as well as based on my knowledge, training, and experience, I believe that HALL transported the Canon EOS Rebel T2i digital camera and images taken with that camera from the Philippines to the United States.

19. OS Triage alerted to over 8,000 files of interest related to child pornography investigations and also recovered thousands of known child pornography images, erotica and child modeling images on the external hard drive that was connected to the Dell laptop. Many of these images depict very young female children, some appearing to be as young as 3-4 years of age, engaged in sexually explicit conduct, to include oral sex and sexual intercourse, with adult men. Many of the images depict young female children who appear Filipino or Asian with adult white men. I have reviewed all of the images that were extracted with OS Triage from the

16 - 23 63 JMC

external hard drive that was connected to the Dell laptop and determined that there are numerous images of child pornography as defined in Title 18, United States Code, Section 2256(8). By way of example, four of the images located on the external hard drive that was connected to the Dell laptop during the forensic triage are described as follows:

- a. **Zero1289** – an image file that depicts a naked prepubescent female lying on a bed with her legs spread. An adult male is kneeling between the prepubescent female's legs and the adult male's erect penis is penetrating the prepubescent female's vagina.
- b. **Bathrm03** – an image file that depicts a prepubescent female performing oral sex on an adult male.
- c. **gracel set38 141** – an image file that depicts a naked prepubescent Asian female wearing only black lace thigh-high stockings lying on a bed with her legs spread. An adult male is kneeling between her legs and his penis is penetrating the prepubescent female's vagina.
- d. **9yo tori – 018** – an image file that depicts a naked prepubescent female lying on her back with her legs spread. The prepubescent female's left hand is manipulating her vagina.

CONCLUSION

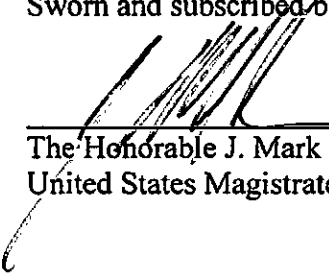
19. Based upon all of the information set forth in this application, I respectfully submit that there is probably cause to believe that Martin Robert HALL violated Title 18, United States Code, Sections 2252(a)(1) (Transportation of Child Pornography) and 2252A(a)(5)(B) (Possession of Child Pornography).

16 - 23 6 3 JMC



Christine D. Carlson
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 8 day of September, 2016.



The Honorable J. Mark Coulson
United States Magistrate Judge

